Final Exam

1. (a) Define the number-theoretic function φ. **(2 points)**

   (b) Solve the equation

$$\varphi(n) = \frac{n}{2}$$

   over the positive integers (i.e. describe the set of solutions). **(4 points)**

Solution. (a) For $n \in \mathbf{N}$, $\varphi(n)$ is defined as the number of residue classes coprime to n, in other words,

$$\varphi(n) = \sum_{\substack{1 \leqslant d \leqslant n \\ \gcd(d,n)=1}} 1.$$

(b) We claim that n is a solution if and only if $n = 2^k$ for some $k \in \mathbf{N}$. To see this is a necessary condition, observe that

$$\varphi(n) = \frac{n}{2}$$

implies that n is even. Assume $n = 2^k p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$, where $p_1, \ldots, p_r$ are odd primes, and $\alpha_1, \ldots, \alpha_r \in \mathbf{N}$ (i.e. this is the canonical form of n). Then, by our formula for φ,

$$\varphi(n) = n \cdot \frac{2-1}{2} \cdot \prod_{j=1}^{r} \frac{p_j - 1}{p_j} = \frac{n}{2} \prod_{j=1}^{r} \frac{p_j - 1}{p_j}.$$

The factor

$$\prod_{j=1}^{r} \frac{p_j - 1}{p_j}$$

is at most 1, and it is strictly smaller than 1, unless it is the empty product. Therefore, there can be no odd prime divisor of n. So the set of solutions is a subset of $\{n = 2^k : k \in \mathbf{N}\}$.

And all such numbers are solutions, either by the formula,

$$\varphi(2^k) = 2^k \cdot \frac{1}{2} = 2^{k-1},$$

or simply by observing that from the set $\{1, 2, \ldots, 2^k\}$ exactly the odd numbers are coprime to n.

2. (a) What is Pell's equation? **(2 points)**

   (b) Solve the equation

$$x^2 - 7y^2 = 1$$

   over the integers (i.e. describe the set of solutions). **(4 points)**

Solution. (a) If d is a positive integer, which is not a square, we call the diophantine equation

$$x^2 - dy^2 = 1$$

Pell's equation. Diophantine means that we look for integer solutions, that is, when $x, y \in \mathbf{Z}$

(b) From general theory, we know the set of solutions can be described the following way. There is a solution (x_1, y_1) such that $x_1, y_1 > 0$ and x_1, y_1 are minimal among the solutions. Let us first find this minimal.

Modulo 7, the right-hand side is 1, and the left-hand side is x^2. The square-roots of 1 modulo 7 are ± 1, so x comes from the set $\{1, 6, 8, 14, 16, \ldots\}$. When $x = 1$, then $y = 0$, and it is not positive. When $x = 6$, then y should be $\pm\sqrt{5}$, which are not integers. When $x = 8$, then we see $y = 3$ is a good choice. By our method, it is clear that this is the minimal solution. Set $x_1 = 8$, $y_1 = 3$

Then all other solutions can be written the following way. For any $n \in \mathbf{Z}$, consider the expression

$$(8 + 3\sqrt{7})^n = x + y\sqrt{7}.$$

Then (x, y) will be a solution. Also, adding signs, $(\pm x, \pm y)$ are solutions, and these are all the solutions, as n runs through $\mathbf{Z}$.

3. (a) Describe those positive integers which are representable as the sum of two squares, and also those which are representable as the sum of three squares. **(2 points)**

(b) Prove that there are infinitely many positive integers which are representable as the sum of three squares but not represenatble as the sum of two squares. **(4 points)**

Solution. (a) A positive integer is representable as the sum of two squares, if and only if each prime number congruent to -1 modulo 4 appears with an even exponent in its canonical form. A positive integer is representable as the sum of three squares if and only if it is not of the form $4^m(8k+7)$ for some m, k nonnegative integers.

(b) For any nonnegative integer l, consider the number $n = 8l + 3$. Clearly it is not of the fordibben form for three squares, since in the equation

$$n = 4^m(8k+7),$$

m must be 0 (the left-hand side is odd, so is the right-hand side), and then $n \equiv 3 \bmod 8$, while the right-hand side is 7 mod 8, excluding equality.

Also, in the canonical form of such a number n, 2 does not appear (since n is odd). Assume the canonical form is

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r} q_1^{\beta_1} \dots q_s^{\beta_s},$$

where each p_i is 1 modulo 4, and each q_j is -1 modulo 4. Since modulo 4, $1 \times 1 \equiv (-1) \times (-1) \equiv 1$, and $1 \times (-1) \equiv -1$, we see that

$$\beta_1 + \dots + \beta_s$$

must be odd. Then at least one of the β's is odd, which excludes representability as the sum of twp squares.

4. (a) State Minkowski's convex body theorem. **(2 points)**
   (b) Assume Λ is a lattice of covolume 1 in the plane. Prove that the minimal distance between two distinct points of Λ cannot be more than $2/\sqrt{\pi}$. **(4 points)**

Solution. (a) Assume $d \in \mathbf{N}$, Λ is a lattice, and B is a convex, compact set which is further centrally symmetric with respect to the origin. If

$$\mathrm{vol}(B) > 2^d \mathrm{covol}(\Lambda),$$

then $B \cap \Lambda$ contains a point different from the origin.

(b) Assume, by contradiction, that this minimal distance δ is bigger than $2/\sqrt{\pi}$ (such a minimum exists, this is not completely obvious, but from the wording of the problem, we can take it for granted). Choose r then such that

$$2/\sqrt{\pi} < r < \delta.$$

Now draw the ball centered at the origin of radius r. Then its volume is

$$r^2\pi > \left(\frac{2}{\sqrt{\pi}}\right)^2 \pi = 4 = 2^2 \mathrm{covol}(\Lambda).$$

Applying Minkowski's theorem about convex bodies, we see that there is a point $p \in B \cap \Lambda$. Then

$$\mathrm{distance}(p, 0) < r < \delta,$$

and this means that there are two lattice points with distance smaller than δ, contradiction.